

► A CONCISE GUIDE
TO THE GERMAN
ePASSPORT SYSTEM
2007



www.bundesdruckerei.de

► A CONCISE GUIDE
TO THE GERMAN
ePASSPORT SYSTEM
2007

ALL ABOUT THE ELECTRONIC PASSPORT

BUNDES  DRUCKEREI

CONTENTS

Foreword by State Secretary Dr. August Hanning (Federal Ministry of the Interior) . . .	III		
Introduction	V		
1. THE ePASSPORT – A TRAVEL DOCUMENT WITH A CONTACTLESS CHIP	1		
1.1 Recommendations by the International Civil Aviation Organization (ICAO)	1		
1.2 Politics as a driving force behind ePassport developments	2		
1.3 The introduction of the German ePassport in two phases	3		
1.3.1 Phase 1 – Integration of facial biometrics	3		
1.3.2 Phase 2 – Integration of fingerprint data	4		
1.4 ePassport infrastructure at the passport authorities	5		
2. THE SECURITY FEATURES OF THE GERMAN ePASSPORT	6		
2.1 The classical security features of German travel documents	6		
2.2 The chip as a new security feature	8		
		3. PROTECTIVE MECHANISMS FOR THE DATA STORED IN THE ePASSPORT	10
		3.1 Basic Access Control (BAC)	10
		3.2 Extended Access Control (EAC)	11
		3.3 Public Key Infrastructures (PKI)	13
		4. DATA PROTECTION AND DATA SECURITY	14
		5. CONCLUSION	18
		GLOSSARY	19
		PUBLISHER'S NOTES	20

DEAR READER,

The ePassport Guide was designed to answer the many queries sent in recent years, not just to Bundesdruckerei as the manufacturer of Germany's electronic passport, but also to the responsible federal department, the Federal Ministry of the Interior. Following the introduction of the first generation of ePassports in November 2005, these queries primarily addressed the specifics of the technical implementation of the EU Directive with a view to passport legislation and other closely related topics, such as the security features of the new documents, data protection and data security.

This guide compiles information showing the complexity of the ePassport project in terms of organization and technology and solutions to pertinent questions. In this context, we had to deal with a two-stage process because after the first biometric feature, the digital passport photo, was introduced, the second-generation ePassports would also include fingerprints starting in November 2007. It should also be clear that parallel to preparing the new documents, it was also necessary to design and roll out a comprehensive infrastructure. The quality assurance software for biometric data and hardware components, such as the ePassport readers at passport offices, are examples of this. Close co-operation between Bundesdruckerei and the Federal Ministry of the Interior and its specialist agencies – the Federal Criminal Police Office and the Federal Office for Information Security – as well as federal-state and municipal administrations made it possible to master this mammoth project. More than four million first-generation electronic passports have been issued in Germany to date.

Staff at Germany's 6,000 passport offices are now getting ready for the second-generation ePassport. We have created the necessary conditions for it by amending the Passport Act and related regulations. Municipal administrations are also already equipped with fingerprint scanners and software for the electronic passport application process. Following pilot projects and successful field testing of fingerprint capture, quality assurance and transmission, I am certain that 1 November 2007 will be a positive date for both document security and Germany as a centre of innovation.



With this ePassport Guide, Bundesdruckerei offers comprehensive information about the project. I would like to express my thanks for this and for the constructive co-operation.

I hope you find this guide interesting and informative reading.

Berlin, October 2007

Dr. August Hanning

State Secretary at the Federal Ministry of the Interior

SECURE PROTECTION AND STORAGE OF IDENTITIES

Starting in autumn of this year, the German ePassport will feature for the first time the data of two of the document holder's fingerprints stored in the ePassport chip. The possibility of directly comparing the live image with the ID data stored in the chip will open up a new dimension as regards the clear link between the document and the document holder and will further enhance the protection of a citizen's personal identity. In November 2005, Germany was the first country to implement phase 1 of the ePassport project according to the recommendations of the ICAO (International Civil Aviation Organization) and the security requirements of the EU, i.e. the integration of facial biometrics and the establishment of the required technical infrastructures in an integrated high-security system. In November this year, we will once again be one of the first countries to protect citizens' fingerprint data via Extended Access Control (EAC) and to anchor phase 2 of the ePassport project in the entire ID process chain.

Special mention must be made here to the pioneering role played by the Federal Ministry of the Interior (BMI) during the quick introduction of the ePassport, as well as its work in European and international committees. Valuable groundwork in the field of ePassport technology and standardisation has been performed by experts from the Federal Office for Information Security (BSI) and the Federal Criminal Police Office (BKA); this work was paramount for the successful implementation of the ePassport projects in Germany and other countries.

Isolated solutions will no longer be able to master the challenges that face us in the future. High-security technology means thinking in terms of interoperable

systems which, from the capturing of data to the manufacturing and personalisation of documents and their verification at access or border control points, mirror what is in fact a closed and internationally harmonised security loop.



With its innovative products and solutions, which are being continuously enhanced through work in countless international committees, Bundesdruckerei is persistently helping to improve security standards world-wide. In autumn this year, when German citizens have their fingerprint data integrated into the chip of the new ePassport, we will have implemented one of the world's most complex security concepts.

With this "Concise Guide to the German ePassport System 2007", we would like to offer you an insight into the technical, legal and organizational preconditions which will be fulfilled by November of this year, so that a smooth application and issuance process will be guaranteed for each and every citizen in Germany. This is our contribution towards significantly improving identity security. At this point, we would like to express our thanks to our partners Infineon Technologies AG and NXP Semiconductors Germany GmbH for their useful and helpful contributions to this Guide.

Berlin, October 2007

Ulrich Hamann
CEO of Bundesdruckerei GmbH



Source: Federal Ministry of the Interior

1. THE ePASSPORT – A TRAVEL DOCUMENT WITH A CONTACTLESS CHIP

► Now that the personal data and photo of the passport holder are stored in an integrated electronic chip, the introduction of the electronic passport, in short ePassport, has opened up a whole new dimension in document security and identity protection. On 1 November 2005, the first phase for the introduction of state-of-the-art ePassports was launched and successfully implemented in Germany.

Starting on 1 November 2007, the contactless chips are to store the data from two of the German passport holder's fingerprints as well.

In recent years, the legal, political and technical preconditions for developing state-of-the-art ePassport systems have been prepared by many international bodies and committees and implemented in the development departments of leading suppliers of high-security technologies. ◀

1.1 The recommendations by the International Civil Aviation Organization (ICAO)

► The international use of travel documents calls for interoperability between the participating systems. If this is to be achieved, the systems and documents used must be standardised accordingly.

For a number of decades, the ICAO as a sub-organization of the United Nations (UN), has set about the task of making travel easier and more secure over time through the standardisation and securing of internationally valid travel documents. The ICAO is also the central institution that addresses new security technologies and biometric methods for travel documents. It develops internationally co-ordinated standards and issues recommendations for optimum handling, security and environmental compatibility in civil aviation. Back in the 1990s, the ICAO had already standardised the machine-readable passport (MRP).

Since July 2005, one focus of the ICAO's work has been the standardisation of electronic components for international travel documents which are defined in Document 9303. This document extensively describes both the technical specifications of the chip and the data structures contained on the chip along with the methods for storing facial images and fingerprints, as well as the methods for generating electronic keys. The ICAO foresees a contactless processor chip as the basic hardware for electronic passports.

In 2001, the ICAO specified the introduction of electronic passports with facial biometrics as the internationally valid standard method in order to boost security in cross-border travel.

Around 110 UN member states have adopted the recommendations of the International Civil Aviation Organization and issue ICAO-compliant machine-readable travel documents to their citizens. All the other member states have issued declarations of intent which they will undertake in order to bring their passports in line with the ICAO-specified security level by April 2010.

This means that in the foreseeable future, all ICAO-compliant passports will feature the identity data, a photo or digital image of the document holder and a two-line machine-readable zone (MRZ) on the so-called data page. Using optical methods, the data can then be computer-checked by authorised instances on the basis of the MRZ and during border control procedures, compared with data in existing databases on the basis of the laws of the country of entry. ◀

1.2 Politics as a driving force behind ePassport developments

▶ The new face of international terrorism, cross-border crime and identity theft have made it urgently necessary to employ all the means and possibilities that information technology offers in order to protect the identity of each and every citizen.

The demand for electronic travel documents with integrated biometric features – which was finally explicitly underpinned by the international community following September 11, 2001 – has given a lasting boost to the development of such technologies. New legislation, such as the "US Enhanced Border Security and Visa Reform Act of 2002", which since October 2004 has been obliging the 27 member states of the Visa Waiver programme to enable smoother visa-free entry into the US by introducing ePassports, has led to a new political direction world-wide.

On 13 December 2004, the European Union's response to the international security situation was Directive 2252/2004 which obliged all EU member states to introduce electronic passports with biometric features.

This EU Directive lays down standards and technical specifications for material and printing methods, as well as for the required biometric data of the new ePassport. By demanding a digitised image as a mandatory criterion, the Directive defines facial biometrics as the standard technology for European travel documents and fingerprints as another biometric standard feature to be integrated in a second phase.

All the EU member states, apart from the UK and Ireland, have undertaken to include the digital passport photo in their travel documents within 18 months of the Directive coming into effect. The data of the two fingerprints of the document holder is also to be integrated into the new ePassport three years after the required security standards have been adopted.

The Federal Ministry of the Interior (BMI) and its subordinate agencies have a major role to play in the swift implementation of ePassport technology. German experts are making a valuable contribution to the work in European and international committees, especially in the field of ePassport technology and standardisation issues.

The "Essen Group" was already founded in 2004, initiated by the BMI, the BSI and German business representatives. The "Essen Group" is an informal and cross-national working group, focusing on new-generation ePassports in Europe. It issues recommendations for experts and decision-making committees and also played a leading role in the development of the "Golden Reader Tool" (read software for electronic documents).

The efforts made by Germany's politicians, including the implementation of the 2006 interoperability test in Berlin, deserve special mention too.

Shortly before the binding deadline for the pan-EU introduction of ePassports, the event demonstrated that the requirements for standardising ePassports were successful and that the technology had been effectively implemented world-wide. ◀

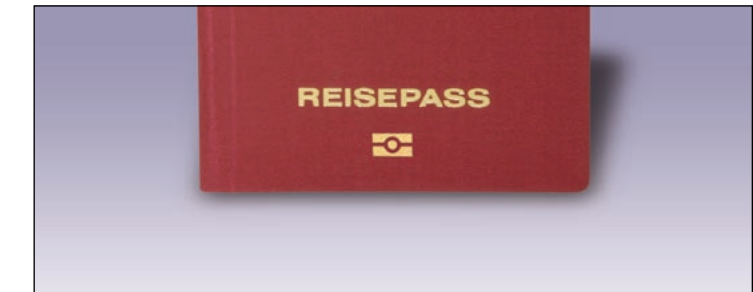
1.3 The introduction of the German ePassport in two phases

▶ Pursuant to the binding EU Directive, the ePassport will be introduced in Germany in two stages. Since 1 November 2005, new German travel documents feature a contactless chip integrated into the front cover of the passport booklet. This chip stores the personal data of the document holder, along with the digital passport photo. The new document can be recognised as an ePassport by the stylised chip symbol on the front cover page of the passport booklet.

1.3.1 Phase 1 – Integration of facial biometrics

In the first phase of introduction, the electronically stored digital passport photo already significantly strengthened the link between the document and the document holder, as well as the possibilities for reliable verification procedures.

Document security was already boosted considerably at the end of 2005 when it became possible to compare the passport photo on the data page with the image data stored in the chip. The additional possibility to compare the stored information 1:1 with the live camera images also paved the way for computer-based identity verification.



ePassport symbol on the German passport

Since only a frontal image permits software-based verification of passport photos, this type of image was defined by the ICAO as the standard for passport photos with biometrics capabilities and/or suitable for biometric verification.

In order to boost image quality, Bundesdruckerei and the BMI supplied the agencies in charge with a photo sample board and a template for the visual verification of passport photos. Furthermore, the agencies received specific verification software which automatically checks to ensure that the facial image scanned complies with the ICAO requirements and passes it on to the next steps of the process. In phase 1, access to the personal data stored in the chip and the stored photo is protected by the Basic Access Control (BAC) mechanism.

1.3.2 Phase 2 – Integration of fingerprint data

Starting 1 November 2007, Germany's passport agencies will capture two fingerprints from the ePassport applicant in addition to the digitised facial image.

During the capture process, the fingerprint data undergoes a software-based quality check. In order to meet the high quality requirements for the data records stored, each fingerprint must be taken three times and analysed so that the best result can be automatically selected. Precise rules determine how individuals with weak fingerprint lines or missing fingers are to be handled in the capture process, so that they too receive a valid ePassport.



Comparison of fingerprint data

The fingerprints taken are automatically compared to each other by placing the co-ordinates of the minutiae (the points where fingerprint lines intersect) from two digital images on top of each other. If the co-ordinates are found to match sufficiently, both images are assigned to the same person and biometric verification is considered successful. This type of verification is the same as the method to be used later in border control checks.

Access to fingerprints is managed by an additional form of access protection called Extended Access Control (EAC). Only authorised countries receive permission, i.e. electronic access authorisation, to read out the fingerprint data.

Just like the facial biometric information, the fingerprint data is stored as a file, encrypted together with all the other application data and then transmitted to Bundesdruckerei, the passport producer, via highly secured communication infrastructures (refer to section 3). The passport producer stores the fingerprints exclusively on the passport chip. After the passport has been produced and has successfully undergone a quality check, the fingerprints are deleted at Bundesdruckerei. The finished ePassport is sent, as usual, to the passport authority where it is ready for the citizen to pick up. Following another quality check by an officer at the passport authority, and if necessary, by the applicant (using an ePassport reader), the fingerprint data is also then deleted from the systems at the passport authority. This means that the fingerprints are exclusively stored on the passport chip. In Germany, it is not permitted to store such data in the passport register or in any other database. ◀

1.4 ePassport infrastructure at the passport authorities

▶ Passport authorities have a central role to play in the application and issuance of travel documents. Integrating the new processes into the workflows of these authorities poses an enormous challenge, not least due to the high number of such authorities – there are around 6,000 passport authorities in Germany equipped with some 17,000 workplaces and featuring a very heterogeneous IT infrastructure. Bundesdruckerei ensures that the tools needed are available at each and every workplace. This means that it was necessary to create complex information and communication infrastructures which warrant secure data transfers and control methods throughout the entire ID process chain.

In phase 1, i.e. with the introduction of passports with a chip and a photo stored as a biometric feature, all the workplaces were equipped with suitable software to ensure the quality of the biometric data. Furthermore, article 4 of Council Directive 2252/2004 states that each document holder has the right to view their data stored in the ePassport chip. This calls for reading devices designed specifically for the technical security features of the document, as well as the procedures specified for access protection of stored biometric data. Bundesdruckerei has equipped all the passport authorities with suitable, easy-to-use ePassport readers.

In phase 2, i.e. when fingerprints are additionally included in the passport, the existing infrastructures will once again be expanded and protected by a host of additional security mechanisms. For this purpose, Bundesdruckerei is supplying fingerprint scanners to all the passport authorities. In addition, Bundesdruckerei is providing all passport authority workplaces with a new

biometrics module for municipal citizen registration procedures which contains the necessary image check and fingerprint scanning functions.

The biometrics module is an extended version of the citizen registration procedure and offers the following biometric functions. It

- checks the biometric capability of passport photos
- displays and outputs the evaluation results
- displays and outputs correction messages
- supplies the evaluation results and quality information for the citizen registration procedure
- automatically compresses the data of the passport photos taken
- captures the fingerprint data
- displays the live image from the fingerprint scanner
- evaluates the quality of the live image
- displays the quality index calculated for the fingerprints taken
- automatically compresses the data of the fingerprints taken.

A smooth application process can be implemented for all citizens thanks to this latest technological method.

In order to be able to read out the fingerprints stored and display these in a manner that ensures the required data transparency, in October 2007, Bundesdruckerei will begin within the scope of the second phase of introduction, to adapt all ePassport readers to the requirements of extended access protection, EAC (refer to section 3.2), beginning with the federal-state capital cities. ◀

2. THE SECURITY FEATURES OF THE GERMAN ePASSPORT

► The German passport is one of the most secure travel documents world-wide. A host of visible and non-visible security features form a barrier that is almost impossible to overcome, protecting the document against counterfeiting or manipulation.

The chip has boosted the security of the ePassport significantly

The integrated, contactless chip and the biometric features stored and protected there have created an additional security feature and clearly link the document to the document holder. ◀

2.1 The classical passport security features (a selection)

► The security level of German ID documents is being continuously examined and adapted to meet the latest demands. Even years before the introduction of state-of-the-art chip technologies, it was possible to once again significantly enhance the forge-proof capability of German passports by integrating holographic security features developed by Bundesdruckerei. With the inclusion of the so-called Identigram®, which is used at various points of the document, the German passport has been setting new national and international security standards since 2001.



Security features of the German passport

1 Identigram® – holographic portrait

A second, holographic image of the passport holder's photograph becomes visible to the right of the conventional picture when the passport data page is viewed from a shallow angle. The holographic reproduction process creates a stylised, light-dark image of the ID photograph's pictorial content into which four motifs of the German eagle are incorporated on the left-hand side.

2 Identigram® – 3D German eagle

A three-dimensional image of the German eagle in red can be seen from a specific viewing angle.

3 Identigram® – kinematic structures

Kinematic structures are arranged above the conventional photograph; their central element is a German eagle surrounded by twelve stars. When the passport data page is tilted from left to right, the eagle motif, which is visible

at the centre, changes to the letter "D" via a hexagonal structure. The stars alternately increase and diminish in size. The hexagons above and below the eagle motif move up and down. A chain of stars on the right-hand edge of the picture turns into the letter "D".

4 Identigram® – macrolettering and microlettering

There are kinematic structures on the left edge of the conventional photograph consisting of a curved band of macrolettering with the text "BUNDESREPUBLIK DEUTSCHLAND" (Federal Republic of Germany); several parallel lines of microlettering with the same text connect with the macrolettering on the left-hand side.

5 Identigram® – contrast reversal

When the data page is tilted, the contrast on the surface of the central eagle motif is reversed, so that the initially bright eagle appears dark on a light hexagonal surface.

6 Identigram® – holographic representation of the machine-readable zone

The machine-readable zone (MRZ) of the data page is displayed as a holographic reproduction. This is situated above the conventional machine-readable zone.

7 Identigram® – machine-verifiable structure

The Identigram® features a machine-verifiable structure. This also enables an automated authenticity check to be made to support visual inspection. This structure does not contain any personal or document-related data.

8 Surface embossing

The data page is embedded into a special laminate. The tactile relief surface with visible embossing contains the letter "D", the German eagle motif and the words "BUNDESREPUBLIK DEUTSCHLAND" (Federal Republic of Germany) and "REISEPASS" (Passport).

9 Security printing with multi-colour guilloches

Guilloches are protective patterns made up of fine, interlacing curved lines in which different-coloured structures fit perfectly to form a balanced overall picture. In reproductions (e.g. colour copies), the line structures of the original are resolved into dotted half-tone structures.

10 Laser engraving

The passport holder's family name and first name are laser-engraved as tactile features into the ID document material at the right-hand side of the photograph.

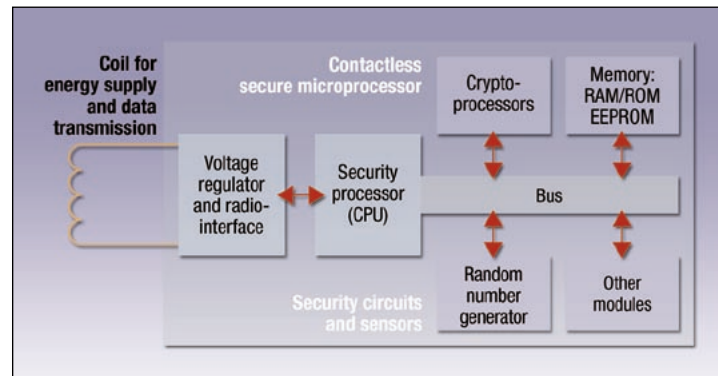
11 Watermark

When light shines through the paper of the passport data page, a multi-tonal watermark becomes visible, showing several stylised eagles distributed over the surface.

Furthermore, the ePassport is produced in special production lines which were specifically designed for Bundesdruckerei using material exclusively manufactured for Bundesdruckerei. The closed production chain guarantees that no non-personalised raw documents exist which could be used for forgeries. ◀

2.2 The chip as the new security feature

► The chip used in the ePassport is a security processor chip (security controller) and hence a mini computer.



Layout of a security controller

Hardware. Taking up just a few square millimetres, the security controller is on a thin silicon disc that controls 64 to 72 Kbytes of memory for the biometric applications of the ePassport, protects access to the data stored in the chip and warrants secure communications with reading devices. The chip and reading device communicate contactless via radio according to the ISO/IEC 14443 standard at a frequency of 13.56 megahertz. The distance between the chip and reading device can range from just a few millimetres to a maximum of 10 centimetres.

The chip generates its operating voltage from radio waves emitted by the terminal unit. Information is passed on to the reader via the modulation of the field strength controlled by the chip. This inductive method, which uses wire coils as antennas, enables data transmission rates of around 100 to 850 kbps. Today, the German ePassport works with a transmission rate of around 424 kbps, thus enabling the quick transmission of the data stored on the chip. The chips used in the ePassport are produced in Germany by the companies Infineon and NXP.

Protective mechanisms of the chip. All the chips used for the ePassport feature robust mechanisms to protect it against external attacks. All the data stored is encrypted using cryptographic methods. The processor continuously monitors its internal operating status and can therefore immediately respond to disruptions during the processing of programs. Special sensors can identify manipulation, e.g. changes in supply voltage, working frequency, temperature or the effects of laser light.

Distribution and further processing. Generally speaking, the manufacturer must protect all its ePassport chips with digital transport keys. In order to personalise the chips in the next step, the corresponding counterpart to the transport key is required. This prevents any unauthorised processes from being performed. Following successful personalisation at Bundesdruckerei, the chip is interlocked, preventing any later modification, amendment or manipulation of chip data.

Security certification. The process chip which is used has undergone various standardised test procedures as required by internationally binding criteria and is classified in the highest security level (Common Criteria EAL5+). Following extensive testing by authorised security labs using the "BSI-PP-0002" protection profile, this classification was confirmed in a certificate issued by the Federal Office for Information Security (BSI).

A T-Systems-developed operating system (TCOS 4.x) on the processor is responsible for ensuring the electronic security of data and the administration of access rights. Based on the "BSI-PP-0026 Machine Readable Travel Document with ICAO-Application, Extended Access Control" and "BSI-PP-0017 Machine Readable Travel Document with ICAO-Application, Basic Access Control" protection profiles developed by BSI, the operating system and the data structure were awarded "Common Criteria EAL4+" certification.

All the production, distribution and personalisation processes at Bundesdruckerei are also the subject matter of security certification by BSI and are strictly monitored and regularly audited. ◀



The German ePassport reader

3. PROTECTIVE MECHANISMS FOR DATA STORED IN THE ePASSPORT

► The data in the chip of an ePassport is stored via a specific file system according to the ICAO "Logical Data Structure" (LDS). The personal and document-related data is also stored in the individual data groups (DG) of this data structure. The following data groups are distinguished:

DG 1 contains the family name and first name, the date of birth, sex and nationality of the passport holder, as well as the serial number of the passport, the ID number of the issuing country along with the document type (e.g. P=Passport) and the date of expiry.

DG 2 contains the facial image of the passport holder.

DG 3 contains two images of the passport holder's fingerprints.

Protective mechanisms communicating with the chip manage authorised access to the data on the chip. The information contained in the DG 1 and DG 2 data groups of the German ePassport are protected by "Basic Access Control (BAC)". The data contained in the DG 3 data group can only be read out via the "Extended Access Control (EAC)" mechanism. Both protective mechanisms are standardised within the EU and are mandatory for the member states. ◀

3.1 Basic Access Control (BAC)

► In Europe, electronic passports with an integrated chip on which the biometric features of the face are stored must at least feature Basic Access Control (BAC) in order to protect them against unauthorised eavesdropping or skimming.

The key function of the BAC method is to ensure that the data can only be read out following successful authentication of an authorised reading device. In this case, the passport holder's date of birth, along with the passport number and the date of validity of the document are first optically read out of the machine-readable zone of the ePassport. Using this information, the reading device calculates a specific access key which authorises the ePassport chip to output a random number and activates the ePassport reader in order to generate the key half that matches the key for the transmission of all the data. Following successful BAC authentication, private keys with

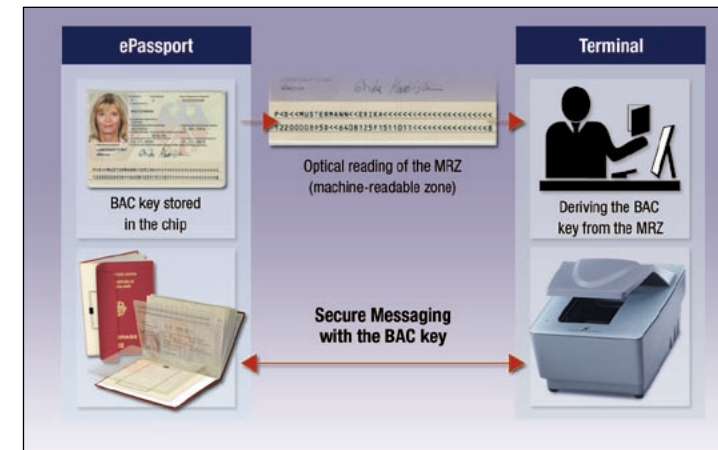


Diagram of the BAC mechanism with chip access

a key length of 112 bits are again exchanged by the reading device and the ePassport chip using standardised cryptographic methods (3DES method). This means that the data is reliably protected against unauthorised access during transmission.

3.2 Extended Access Control (EAC)

► Extended Access Control (EAC) was developed on behalf of the Federal Ministry of the Interior (BMI) under the leadership of the German Federal Office for Information Security (BSI) in order to protect the fingerprints to be stored in German ePassports starting 1 November 2007. A much higher level of security is warranted by EAC. The EAC method is the mandatory security standard for all EU member states when it comes to storing fingerprints.

In terms of data protection requirements, EAC offers two key advantages:

1. EAC uses additional protective mechanisms to secure the process of reading out fingerprint data,
2. EAC permits the assignment of selective access rights, so that only authorised readers have access to the fingerprint data.

Germany will be one of the first EU countries to implement the second generation of ePassports and hence use EAC for the first time in a sovereign application. Bundesdruckerei has already demonstrated the suitability of the EAC method. During the 2006 World Cup football championship, this method was used in a large-scale application in the "adidas world of football" arena in Berlin.

Now that almost all EU member states have undertaken to issue their citizens' ePassports with fingerprints, this standard will gradually become established throughout Europe and in many non-European countries.

What does EAC mean?

EAC generally manages access rights to the fingerprint data stored in the second-generation ePassport. Based on a special electronic access right, the reading device, like the one used at border controls, receives permission to read out the fingerprint data. It is not possible to read out the data without such an access certificate.

Within the scope of the EAC mechanisms, each authorised reading device must have its own key pair which can be verified by the chip in the passport. Furthermore, it also has its own electronic certificate which defines the specific rights of the reading device.

Which specific access rights are to be assigned to the authorised reading device is determined solely by the country issuing the passport. This means that the respective national Certification Authority (CA) exclusively determines which data groups are to be accessed and by whom. In this way, certain countries can be denied access to the fingerprint data of a German citizen.

The real core of EAC technology is hence certificate-based authentication which enables the checking of authorised access as well as the authenticity of the integrated ePassport chip. This method is implemented using asymmetric, cryptographic mechanisms which are based on interaction between the public and private keys. Once the chip and terminal have been successfully authenticated (see below), BAC-based, encrypted communication is triggered between the reading device and chip, while stronger session keys are used once again. ◀

The following steps are carried out in succession in an EAC process in order to read out all the data stored in a state-of-the-art ePassport, including the fingerprints:

- **Step 1:** Following successful Basic Access Control (BAC), access is possible to the personal data and the digital facial image.
- **Step 2 :** Prior to the so-called chip authentication process, the chip proves that it is not forged or copied. For this purpose, cryptographic methods are used in the encrypted communication between the ePassport and reading device in order to establish an asymmetric key exchange mechanism. Only an "authentic" chip (i.e. a chip which has its own key pair and where the public key is certified) is capable of communicating with the reading device. This automatically ensures reliable protection against copying for the stored data contents. Successful authentication of the chip warrants the authenticity of the document.
- **Step 3:** With the help of a terminal authentication process, the reading device must now prove its identity as a unit authorised to access and read out fingerprint data. For this purpose, the authentication certificate of the reading device is checked during communication between the chip and reading device. In Germany, the BMI issues sovereign certificates, exclusively determining who and which devices are to have access to fingerprints. These certificates have a limited period of validity. The required certificates are made available via a public key infrastructure (PKI).
- **Step 4:** Communication between the reading device and chip is encrypted and is based on the "3DES method", already used in the BAC mechanism together with high-quality session keys.

Since the certificates required to access fingerprints are issued by individual countries, the following scenarios are conceivable for future international travel:

- Countries which have not adapted their reading devices for chip technology will check passports in the conventional way, i.e. visually and/or by scanning the machine-readable zone (MRZ).
- Countries which do not receive certificates authorising them to read the fingerprints but do have systems to read ePassports can only read out the biometric data of the facial image from the chip and use this for biometrics-based eChecking.
- Countries which have the necessary certificates can also read the traveller's fingerprint data.

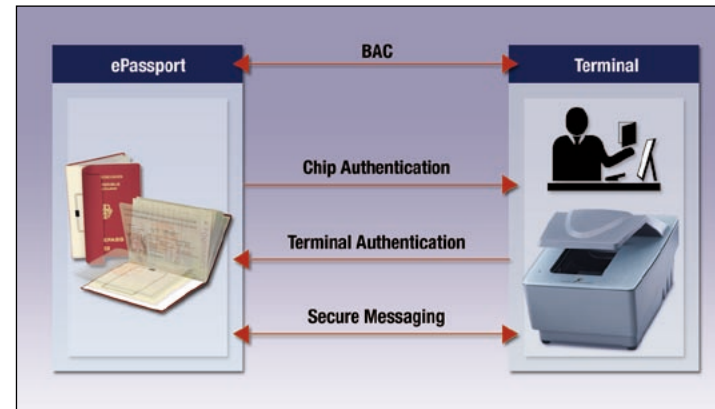


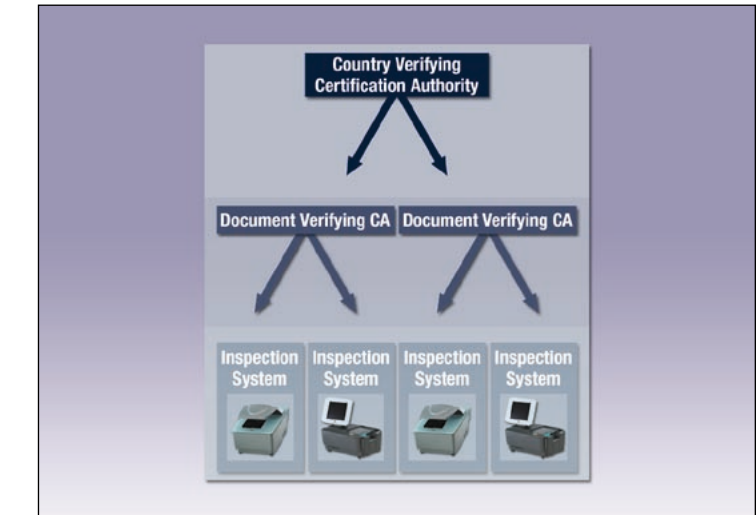
Diagram of the EAC mechanism with chip access

3.3 Public Key Infrastructures (PKI)

► Access rights to the entire data record of a second-generation ePassport can be restricted to a certain device or limited to a certain period of time. It must also be possible to reliably distribute and assign such rights even in inhomogeneous infrastructures; for instance, devices at embassies, airports, or in mobile applications.

The EAC method uses a two-level PKI to master this complex distribution procedure: The supreme issuing authority for sovereign national certificates is the Country Verifying Certification Authority (CVCA). This authority issues authorisation certificates to the second level, the so-called Document Verifying Certification Authority (DVCA). From this level, the valid certificates are distributed to a pool of reading devices and the access rights are managed. Based on the access rights for documents assigned by the DVCA, the inspection systems of the document reading devices can then control the required reading and checking procedures. This method is currently only valid for access rights within one country.

If a state wishes to provide another state with access to "its" citizens' fingerprints for control and security purpose, this then calls for a much more complex EAC method. This is because the different national Country Verifying Certification Authorities now have to additionally exchange and manage authorisation certificates between each other.



3-level EAC public key infrastructure

EAC is an extremely complex topic and only a select number of suppliers of high security systems are capable of professionally steering and implementing it in all sub-areas. Bundesdruckerei ensures that national eDocuments are interoperable in international border traffic and, together with its subsidiary D-TRUST, one of the first certified trust centers in Germany, provides the infrastructures required for the German ePassport project. ◀

4. DATA PROTECTION AND DATA SECURITY

▶ Two aspects must be distinguished when it comes to data protection and data security for electronic passports:

1. The question concerning the storing and use of data in general

2. The security of the data stored in the ePassport chip

A host of data protection and data security regulations have been agreed to on a European level, especially with a view to rules governing the use and securing the integrity, authenticity and confidentiality of the data. In this context, the proposals tabled by the working group of data protection commissioners from all EU member states (pursuant to article 29 of the EU Data Protection Directive) have been largely included in the EU's draft regulation.

As regards national passport legislation, Germany has gone far beyond European data protection requirements. Contrary to many other EU member states, Germany will not have a nation-wide database with biometric data. The passport data and photograph will be exclusively stored in the municipal passport register. The fingerprints are then deleted after the passport has been issued by the passport authorities.

The ePassport is a travel document. This means that the most important and explicitly desired function of the chip is its ability to be read at border controls and the possibility to establish an unquestionable link between the document and the document holder through an automated 1:1 comparison of the biometric data.

At the same time, any unnoticed reading of the chip contents by unauthorised parties must be reliably prevented. This is why the security properties of electronic passports are designed to facilitate the required smooth and reliable reading for authorised control purposes, as well as the warranting of the data protection required by law for the citizen.

Data transparency. At the passport authority, citizens can always view the data stored in their ePassport chip using special display devices, the ePassport readers. The following data is displayed:

- **personal data:** first name and family name, date of birth, sex and nationality of the document holder,
- **document-related data:** serial number, issuing state, document type and expiry date,
- **biometric data:** a digitised facial image, two fingerprints.

Data security. The level of security for the data stored in the chip has been agreed upon in international and European committees and has been adopted throughout the EU as a binding security requirement. Based on this:

- all the data stored on the chip must be electronically signed, so that any attempt to change it does not go unnoticed,
- once personalised, all ePassport chips must be blocked against any further write access,
- all ePassports throughout Europe must be protected by the BAC and EAC mechanisms against unauthorised access.

The BAC and EAC access protection methods were extensively shaped by German experts from Germany's Federal Criminal Police Office (BKA) and the Federal Office for Information Security (BSI).

Protection against attacks

Despite these far-reaching security precautions, the fear of unauthorised access and/or criminal acts, such as identity theft or document forgery, continue to be an important topic for Germany's citizens, also in conjunction with the new ePassports.

For this reason, the following section will briefly address some of the most frequently discussed attack scenarios from the perspective of security technology:

- Unauthorised reading of the chip contents
- Changing of the digital data in the ePassport
- Cloning of the digital data in the ePassport
- Creation of movement profiles
- Eavesdropping of communications between the ePassport and the inspection device.

Unauthorised reading of the chip contents

The basic functionality of an interoperable travel document is the verification of the optically readable data in the passport (identity data, passport photograph and machine-readable zone) and the data stored in the chip. Each border control officer must be able to use this data to verify the identity of the passport holder. At the same time, it must be ensured that access to the machine-readable and chip-based data is not possible without the consent of the passport

holder (wilful act of authorised reading), e.g. when the closed document is stored in pockets.

These two basic assumptions form the foundation for the BAC and EAC protective mechanisms. Extensive testing was carried out by independent test laboratories to examine the correct and robust implementation of the described protective measures on the ePassport; this was confirmed by BSI.

Which steps would an attacker who is NOT in possession of the readable information but who still wishes to gain access to the digital data of a passport which is, for instance, closed and carried in a coat pocket, now have to take?

First of all, the attacker would have to come within a few centimetres of the ePassport because this is the distance within which communication with the chip is possible. The laws of electrodynamics dictate that the chip of an ePassport, with its rather small antenna and low power consumption, can only be realistically activated without errors and triggered for communication over distances of less than around 25cm. When longer distances are bridged, the power required increases exponentially. At the same time, the longer the distance between the passport and the reader, the higher the error rate. This is due to existing background noise which then leads to bit errors in the transmission and thereby incorrect data at the reader.

Despite the difficulties described, let us assume that the attacker has managed to establish such a contact without being noticed. If the attacker does not have the data printed on the data page in the passport, then he will have no choice but to test all possible key variants. The attacker can do this

by assuming hypothetical data, generating the BAC-specific keys from this and then executing the basic access protocol. If the ePassport accepts the key generated, this means that the attacker has guessed the correct data and can gain access to the digital photo.

Estimating how long an attacker needs to guess the correct key is of major importance when it comes to determining the security level and suitability of the method. The number of attempts required depends heavily on the total possible number of key variants. Even if part of the information is correctly guessed or is already known, the latest analyses by BSI show that 12 days would still be needed in order to guess "only" six numbers of the key required.

The physical presence of the passport near the perhaps disguised reading device is needed to perform the attack practically. In other words, reading the digital data "in passing" is not realistically possible. The decisive limiting factor is the chip in the ePassport itself. A single attempt to access an ePassport using the BAC mechanism takes approximately 1 second. Even using high-performance computers in the background, an attacker would not be able to accelerate the attack process, as only the ePassport itself can confirm in its response that the hypotheses made by the attacker were correct.

If an attacker has more information, he will probably already have a copy of the data page of the passport booklet in question. This means that the amount of additional information to be gained by reading the chip is relatively limited. Even a high-quality photo of the target person can be taken without any risk over a long distance and with simple technical means, such as a camera.

In the case of the approach presented, we are referring only to the data protected by BAC which is visible on the passport data page anyway. If an attacker also wants to access the fingerprint data secured by EAC, he would not only have to overcome the BAC mechanism, but would also have to prove his authenticity and authorisation within the scope of the EAC protocol.

However, the asymmetric key pairs are exclusively issued as certificates and digitally signed by the authorised bodies, such as the Country Verifying Certification Authority (CVCA) and the subordinate Document Verifying Certification Authority (DVCA). This means that the entire high-security environment of the High Security Module (HSM) would have to be bypassed; from a security technology perspective, this can be ruled out in today's PKI infrastructures.

Changing the digital data stored in the ePassport

If optically readable passport data is changed, the data stored in the chip must then also be changed, since any deviation between the optical and digital data would be immediately noticed during verification.

The digital passport application specified by the ICAO and the EU that is available on the chip is designed in such a manner that only reading access is possible in practical operations. The configuration ensures that the write mechanisms which are used to enter the personalisation data into the chip are no longer available once the document has been issued.

Furthermore, the chip components themselves used in the ePassport feature generic security mechanisms which automatically ensure the confidentiality and integrity of the data stored on the hardware level, as well as the recognition of external manipulation. Regular evaluation and certification ensure and confirm

the efficiency of these mechanisms. This prevents manipulation of the digital data both on the application, as well as on the hardware level.

In addition to this, all the data stored is secured by digital signatures. The key lengths of the authorised Document Signer are so long that even if all the computer capacity available world-wide were used, it would not be possible to guess the private keys.

"Cloning" the data stored in the chip

"Cloning" is understood to be the transfer of the data read out of an ePassport to another chip. In this context, it must be noted:

1. As explained above, the data cannot be read out without authorisation.
2. It is not possible to change/manipulate the data on the chip.
3. The chips of the second generation of ePassports are basically not "cloneable", because the private keys used in the chips are not disclosed even if a reading device with sovereign authorisation is used.

Recording contactless communication

The BAC protocol forces the encryption of the information exchanged via Secure Messaging, i.e. it ensures the confidentiality and integrity of the digital information exchanged using session-specific, symmetric keys based on the triple-DES method. The longer the distance between the reading terminal and the recording device, the weaker is the signal and the higher the error rate. As the signals become weaker, the error rate rises. This means that it is practically impossible to record contactless communication.

Even if information is recorded, it would have to be successfully decrypted before it can be accessed.

Creation of movement profiles

A chip which operates in contactless mode generally makes information available at different levels. This information is required in order to establish the contactless protocol required by the ISO 14443 standard.

An ePassport, which, like the German ePassport, is certified according to the "MRTDs with BAC Application" protection profile, generates a session-dependent, changing, random identifier each time the ePassport is accessed. Unlike a mobile phone, which always sends the same identifier and therefore enables the creation of movement profiles, this is not the case with the ePassport.

Attackers who are interested in precise movement profiles of certain target individuals have much easier methods at hand (e.g. the use of the data recorded by mobile phone companies) than the difficult route presented by highly protected ePassports. Therefore, attacks of this kind do not make any sense. Further, practical implementation would also be impossible because the equipment and effort needed to evade the security features of the chip would be too complex. ◀

5. CONCLUSION

► Secure storage and immediate availability of personal data and information is one of the fundamental needs of modern life. Travel and international exchange along with safe and unrestricted mobility all over the world created the need for new technical security solutions. With the advancement of globalisation, these solutions became necessary for international border traffic as well. The simple ID "paper" has long since ceased to comply with national and international security standards. A host of highly complex security systems are needed to protect an individual's data identity and to establish a reliable connection between the holder and his or her ID document.

With the introduction of the second-generation ePassport on 1 November 2007, Germany will be one of the first countries in the world to achieve a new dimension in identity security for its citizens. The fact that this new milestone is being monitored circumspectly and questioned is both necessary and right as far as reliable data protection is concerned.

The two years which have passed since the launch of the first phase of biometric-based, electronic ID documents have been put to good use with a view to security technology and data protection legislation. The existing

infrastructures, the security and protective mechanisms, as well as methods to ward off possible attacks were once again optimised significantly. This means that German document holders are currently warranted the highest conceivable level of identity protection and document security.

The new ePassport technology marks a quantum leap in security. The challenge we now face is to maintain and enhance this further.

Matter-of-fact, open and critical dialogue will also help us to achieve our common goal, i.e. to uphold and protect the identity of each and every citizen through reliable ID processes and systems; not just today but also in the future. ◀

GLOSSARY

BAC	Basic Access Control – access protection for data stored in the ePassport
CSCA	Country Signing Certification Authority – the supreme body of a Public Key Infrastructure for the personalisation and verification of ePassports
CVCA	Country Verifying Certification Authority – the supreme body of a Public Key Infrastructure for performing Extended Access Control
DES	Data Encryption Standard – a symmetric encryption algorithm
DVCA	Document Verifying Certification Authority – a body to transmit access authorisations to those reader units which are authorised to access the fingerprints stored in the ePassport
DG	Data Group – the Logical Data Structure (LDS) is subdivided into data groups. They include, for example, the fingerprints or the facial image
EAC	Extended Access Control – extended access protection for the fingerprints stored in the ePassport
HSM	Hardware Security Module – computer components for storing data and generating keys

ICAO	International Civil Aviation Organization
IS	Inspection System ("reading device") – document reader and verification units, for example at registration offices or border control points
ISO	International Standards Organization – the supreme international standard-setting body
Inlay	Comprises the chip module, the antenna and the support material and is used as a component for the production of smart documents (such as smart cards or ePassports)
LDS	Logical Data Structure – this standard describes the way data is stored in the chip of an ePassport
MRP	Machine Readable Passport
MRZ	Machine Readable Zone – the machine-readable lines on an ePassport used for reading the details via OCR
MRTD	Machine Readable Travel Document
PKI	Public Key Infrastructure – the technical infrastructure for the distribution of keys and certificates
RFID	Radio Frequency Identification – process for automated, contactless identification of objects and individuals
Triple-DES, 3DES	A method of increasing the security of DES by encrypting three times with different keys

CONTACT

Bundesdruckerei GmbH · Oranienstrasse 91 · 10969 Berlin, Germany

Phone +49 (0) 30 - 25 98-0 · Fax +49 (0) 30 - 25 98-22 05

E-mail Info@bdr.de · www.bundesdruckerei.de

Published by Bundesdruckerei GmbH, Oranienstrasse 91, 10969 Berlin, www.bundesdruckerei.de

Copyright © 2007 Bundesdruckerei GmbH, Berlin